International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 4326~4335
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp4326-4335

Novel model for boosting security strength and energy efficiency in internet-of-things using multi-staged game

Bhagyashree Ambore, Suresh L.
Department of Computer Science and Engineering, Cambridge Institute of Technology, India

Article Info

Article history:

Received Aug 8, 2018
Revised Apr 15, 2019
Accepted Apr 30, 2019

Keywords:

Attacks
Energy
Game theory
Internet-of-things
Security

ABSTRACT

Security as well as energy efficiency is one of the most inevitable and challenging problems when it comes it large scale network deployment like INternet-of-Things (IoT). After reviewing existing research work on IoT, it was found that there are discrete set of solution for security as well as for energy. However, there is little research work that has jointly investigated both the problems with respect to IoT. Apart from this, there are also various form of attacks that cost energy of sensors that constitutes core physical devices in IoT. Therefore, these manuscripts present a novel idea for identifying and resisting the security breach within an IoT system ensuring energy efficiency too. Harnessing the modelling capability of game-theory, the proposed system offers a joint solution towards these problems. The simulated outcome of the study is found to offer balance performance for better energy efficiency and robust threat mitigation capability when compared with existing approaches.

Corresponding Author:

Bhagyashree Ambore,
Dept of Computer Science and Engineering,
Cambridge Institute of Techbnology,
Chikkabasavanapura, Krishnarajapura, Bengaluru, Karnataka 560036, India.
Email: lsntl@ccu.edu.tw

1. INTRODUCTION

Internet-of-Things (IoT) offers a large chain of connection among different forms of physical system that finally leads to a robust cyber-physical system [1]. Owing to formation of networking among different number of heterogeneous physical devices over various communication strategies, therefore, designing a generic security solution is not feasible in IoT. At present, the security system of IoT focuses on securing either application layer, or transportation layer, or perception layer [2]. There are also different review studies carried out towards addressing security protocols in IoT [3-7], however, there are various questions that are yet left unsolved from the approaches in existing security solution. The first question will be –is there any good alternative for strong encryption mechanism? The second question will be why the existing security solutions are so attack specific. Owing to the novel nature of the technology, answers to such question are yet to be explored. If this answers were ever found, than then next question will be why the researchers have not emphasized on their solution by considering energy factor.

The IoT devices are usually wireless and low-powered hardware which cannot execute complex security protocols. Hence, existing attacks e.g. denial of service, Sybil attack, routing attack, as well as many other unknown attacks too cost the network resource as well as node battery just to resist it. Moreover, there are various types of attacks that are only meant for energy depletion [8]. Just like security problems, the problems associated with energy also exists at present. Recent review work e.g. [10] offers concrete information about different forms of energy efficiency techniques. But unfortunately, none of the existing studies on IoT have ever associated energy problems with security problems.

It is known very well that sensors constitute a major part of the physical devices in IoT which works on the principle of radio-energy model [10]. According to this principle, it is stated that every communication process is directly linked up with the allocated energy from its battery. This energy demands are very often overlooked even in the area of sensory application as they are focused on small-scale implementation and not much on large scale implementation. The demands of energy efficiency is not much on small scale as compared to large scale of deployment e.g. in IoT. Therefore, it is necessary to develop a comprehensive and lightweight protocol that can balance both the energy needs as well as security demands of IoT. At present game-theory is one of the widely accepted modeling concepts that is capable of framing up a complex problems too. The proposed system harnesses this potential for modeling.

Hence, this paper presents a novel technique where game theory has been used for modeling a simple decision making framework with capability of isolating compromised IoT devices. Section 2 discusses about the existing research work followed by problem identification in Section 3. Section 4 discusses about proposed methodology followed by elaborated discussion of system design with respect to assumption & dependencies, algorithm construction strategy, and algorithm implementation in Section 5. Comparative analysis of accomplished result is discussed under Section 6 and conclusion in Section 7.

The problems associated with IoT are many and there are different researchers addressing different problems associated with it. This section briefs of literatures towards security as well as energy problems in IoT. As majority of the IoT devices are using sensors, therefore, there is a deep relationship between the security features and energy efficiencies. The present state of literatures has been witnessing mainly fundamental discussion focusing over the theoretical aspect of IoT (e.g. Wolf and Serpanos [11], Bertino et al. [12], Singh et al. [13], Bhattarai and Wang [14], Burg et al.[15], Nurse et al. [16], Szymanski [17] etc.).

These review literatures assists to introduce various updates techniques presented by different reearchers emphasizing on different techniques.A unique study has been presented by Xu et al [18] where ontology has been used for modeling network threats over IoT. The study has also formulated various rules and reasoning mechanism to resisting security threats in IoT. Security problems could also be solved using software defined network where integer linear programming was proven to be best approach to solve the problem (Liu et al. [19], Villari et al. [20]). Such security features could be further upgraded by enhancing conventional digital signature (Mughal et al. [21]). Apart from digital signature, symmetric encryption, other hashing mechanism, and public key encryption are also found helpful in resisting low end threats over IoT devices (Pereira et al. [22], Raza et al. [23], Xiao and Yu [24]). It was also seen that usage of homomorphic encryption could increase the privacy feature in IoT devices (Song et al. [25]). Apart from encryption, it also improves performance of recryption too. Usage of game theory has been reported to assist in modeling solution towards learning and resisting threat (Wu and Wang [26]).

Another unique study was presented by Zhang et al. [30] where potential of public key encryption has been claimed with lesser size of secret key. Existing literatures have discussed various studies towards securing physical layer in IoT (Hu et al. [27]) by adding artificial noise. Security-based connectivity between IoT and upcoming industry 4.0 is quite high.

A recent study shows that Hidden Markov Model could be used for constructing intelligence to resist security breaches in IoT applications working on Industry 4.0 (Moustafa et al. [28]). The most advanced version in cryptography called as blockchain is recently investigated by many researchers and were claimed to offer potential resistance for IoT devices (Qu et al. [29]). There are also some recent works being carried out towards energy efficiency in IoT using different approaches. It was seen that optimization-based approach assists in developing energy-aware modeling for IoT with better quality of service performance too (Alsaryrah et al. [30]). Work carried out by agah et al. [31] and Hamdi [32] have also emphasized on strengthing security features in IoT.

Another optimization-based approach was introduced in existing system for addressing position-based problems with power control management of uplink transmission (Mozaffari et al. [33]). Discussion about energy-based communication system using sensors has been carried out most recently by Roy et al. [34]. The authors have presented a solution that is meant for energy-efficient routing operation to offer increased packet forwarding performance and increased network lifetime. Hardware-based solution is also presented most recently with an aid of Rectenna. The study carried out by Shafique et al. [35] have shown that energy harvesting can be realy fruitful when worked along with Rectenna. Apart from this, researcher e.g. Bisadi et al. [36], Caruso et al. [37], Mansilla et al. [38], Zhai et al. [39], and Ju et al. [40] have also emphasized on energy problems in IoT. Therefore, it can be seen that there are different set of literaures towards solving security problems and energy problems very discretely while no connectivity has been established till date between them in IoT. Riahi and Riahi [41] have discussed about game theory for resource distribution in a huge allocated techniques. Sahnoun et al. [42] presented a model called A Coalition-Formation Game model for power efficient routing in MANET. Ahuja and Bedi [43] have developed a technique which is semi blind digital watermaking technique using for video developing MPEG-2 standard.

The study outcomes of above discussed literatures have presented solution for some of the potential security threats and energy problems differently and it was found claiming its successful operation using numerical validation. However, apart from advantages, there are certain associated limitations that are briefly highlighted in next section followed by discussion of the proposed solution to address such problems.

From the prior section, it can be seen that existing research techiniques has distinctive focus on security problems as well as for energy problems. However, the possible connectivity between security and energy problems is very few to find from existing literature. The fact that existing security protocols uses complex encryption technqiue that required higher resource dependencies are not inestigated by existing researchers. At the sametime, energy efficiency approaches doesnt have any consideration of the security features leading to a big trade-off between security and energy problems in IoT.Hence the problem statement is "*Designing a non-cryptographic solution that bridges the trade-off between security and energy efficiency among the IoT nodes is a computationally challenging task*". The next sections briefs of proposed solution.

The core goal of proposed system is to resist all sorts of attack in IoT that makes the devices deplete its energy. The proposed system aims for introducing a novel, simple and yet robust framework that is capable of identifying and isolating the compromised IoT devices considering the fact that there is no predefined information about the threat.

The proposed system implements game theory concept that allows the IoT device to perform certain vulnerability calculation from its neighboring node, assuming that it doesn't know the intention of its neighbor node as shown in Figure 1. Using probability concept and depending upon the extracted information of vulnerability as well as legitimacy, the proposed system makes a decision to isolate all the active connection from any compromised IoT device. By doing this, only the necessary amount of energy is spent to cater up data packet forwarding process. Hence, proposed system is capable of resisting any forms of threats towards active communication process in IoT. The next section briefs about the algorithm implementation for this process.

Figure 2 highlights the system architecture which exhibits that proposed system a game logic based on which it formulates both unique and discrete set of actions to be executed by normal and malicious node. The system performs analysis of vunerability and legitimacy of the node in compliance of sequential rationality of multi-staged game followed by identification of intruder and prevention strategy. The illustration of system design is carried out in next section.

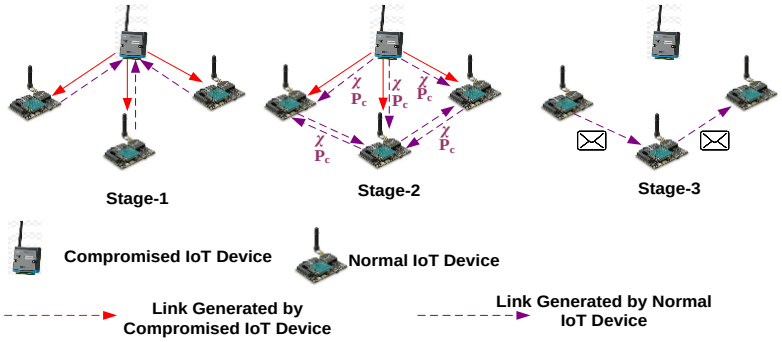

Figure 1 Communication establishment in proposed system

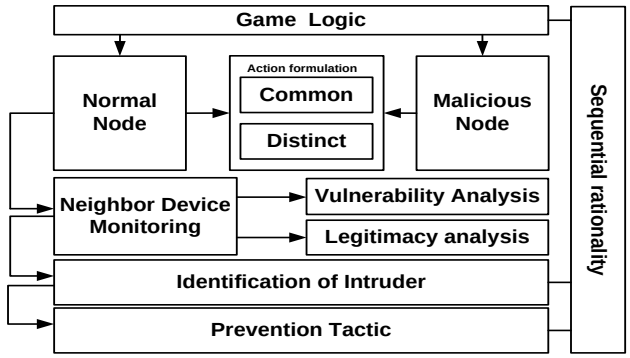

Figure 2 System architecture

2. SYSTEM IMPLEMENTATION

The proposed system aims for constructing a novel decision making mechanism using game theory that offers an enhance intelligence among the IoT nodes to capture the latent behaviour of the malicious IoT nodes. In compliance of the game theory concept, the system design implements multi-staged game to assess the robustness and sustainailty of the proposed concept toward identifying the intrusion as well as intruder. This section discusses about different essential information considered to implement the proposed system.

2.1. Assumption & dependencies

The prime assumption of the proposed system is that it offers a complete independence from any apriori information about the attacker. No normal node is assumed to posses any distinct information about the malicious node. The prime dependency will be that in order to find out the presence of attacker node in its transmission proximity, the normal node will need to perform neighborhood monitoring.

2.2. Algorithm construction strategy

The prime construction strategy of algorithm is that it considers node-A as transmitter node and node-B as receiver node. As there is no apriori information about the malicious node; therefore, each IoT nodes will be required to calculate the degree of secureness and vulnerability. It does so by monitoring two essential information e.g. B_1 and B_2 i.e. total number of packets transmitted and total number of packets dropped. This is because this action can be belonging to both normal and malicious node. Hence, the proposed algorithm design makes a very clear statement of set of actions formulated in multi-staged games i.e. $A=\{A_1, A_2, A_3, A_4\}$,where A_1, A_2, A_3, A_4 will represents when the node choose to forward data, drop data, raises an alarm about malicious node, and launch an attack respectively. A closer look into this set of actions will show that A_3 and A_4 are the only discrete action that represents specifically normal IoT node and malicious IoT node respectively. The algorithm also consider that each player (or IoT nodes) will be executing their set of action one after another and not at a same time.

2.3. Algorithm implementation

The prime purpose of the proposed algorithm is to identify the presence of the malicious IoT node in the network of smart city. The algorithm implements the logic of game theory in order to execute sequential rationality for both normal and malicious node. This is done in order to assess the power of withstand the adversary in presence of potential and unknown attacker. The algorithm takes the input of *n* (total number of IoT nodes) and *A* (simulation area) that after processing leads to identification of vulnerable IoT node. The steps of the proposed algorithm are as follow:

Algorithm for capturing vulnerable IoT node
Input: *n*, *A*
Output: identification of vulnerable IoT node
Start
1. *init* n, A
2. rand(uni(*n*))→*z*
3. **For** *z*=1:*m* |m is maximum number of zone
4. **While** mon(data)<threshold **do**
5. **If** *vul*<cost(data_trans) **then**
6. Select A_1 and opt $p_1=1$
7. **Else**
8. Select A_1 and opt $p_2=\Delta A_4$
9. **End If**
10. Update vul_{param} and compute χ
11. **End While**
12. Idenitify node-*A* as compromised IoT node
13. **End For**
End

The step-wise discussion of the above algorithm implementation is as follows: The algorithm formulates different number of transmission zones z within the simulation area very uniformly (Line-1) which is a direct representation of a categorized transmission area within a smart city. All the normal nodes are then distributed randomly in complete simulation area A in such a way that uniform numbers of IoT nodes are deployed in all the transmission zones z (Line-2). It will also mean that $z=(z_1, z_2, \ldots..z_k)$, where *k* represents $k=n_r \times n_c$ (n_r=number of rows, n_c=number of columns, and $(n_r, n_c) \subseteq A$. The proposed computation

towards exploring and confirming the presence of malicious node is carried out for all the communicating nodes within z (Line-3). The algorithm than executes a monitoring function *mon*() considering the input arguments of *data* (Line-4). Basically, the monitoring function *mon*() computes scalar product of two entities, where the first entite is related to probability of compromised IoT node i.e. P_c and second entity represents non-vulnerable events. The vulnerability in the proposed system is defined as the event of monitoring during which the monitoring node (source node) is not able to confirm the legitimacy of the other node being monitored. However, in order to compute vulnerability, the proposed system is required to compute two essential parameters i.e. B_1 and B_2, while doing neighborhood monitoring using probability function. These parameters are basically utilized for computing positive legitimacy P_L as well as negative legitimacy of the monitored node. The positive legitimacy P_L is calculated as B_1/B_1+B_2 while negative legitimacy N_L is computed as $(1- \chi)-P_L$. Further, using probability, the computation of χ is carried out in the form of function $f(B_1, B_2, c)$, where c represents a network coefficient. A closer look into the formulation of PL $(B_1/(B_1+B_2).(1- \chi))$, $N_L((1- \chi)-P_L=(B_2/B_1+B_2).(1- \chi))$, and χ will show that P_L is never enough to ascertain the legitimacy of the node if $B_1=B_2$. This will mean that P_L will always have a same value in case of $B_1=B_2$. Therefore, the parameter of vulnerability χ assists to offering more disclosure about the legitimacy-baed information about the vulnerable node.

Applying the concept of sequential rationality in game theory, a regular node will always attempt to increase its payoff by capturing more information about the malicious node while the malicious node will attempt to invoke lethal attacks as many as possible. The idea is to observe if the proposed system is actually able to capture such dynamic information using game theory. Therefore, to make the process slightly practical, the study consider threshold of vulnerability and chooses to compare with the monitor data (Line-4). This is possible because if the user adopts a specific application of IoT, they will be aware of the situation of adversaries and non-adeversaries. Hence, user can initialize the value of threshold depending upon the criticality of their application being running over IoT.

The next step of the proposed algorithm is to further compute the degree of vulnerability on the basis of data transmission. The proposed system makes it practical by associating cost with the data transfer. The prime logic implemented here is – every communication task has consumption of specific set of resources (called as cost) for both normal as well as malicious node. This will mean that for every action of attacker, there is a cost associated with it.

Again, based on the concept of sequential rationality, an attacker will never want that their cost of attack should increase and instead should look for more profit to be made by launching an attack. Therefore, the attacker node will not launch its malicious codes in the beginning which will result in increase of trust level of the attacker among the normal nodes and hence it will exhibit A_1 and A_2 actions that are nearly same as that of normal node. However, attacker will not choose to continue exercising this action for long as it will be against sequential rationality rule in Bayesian game. They will stop executing A_1 and A_2 until they find that they can make more profit by launching an attack in comparison to cost to be beared by them for launching that attack. So, the proposed system computes anticipated cost of transmission of data packet by using probability theory (Line-5). For that, it first obtain the total outcome which is a summation of total cost as well as profit involved in the making the data transmission. It then computes the favorable outcome which is the difference of profit for making the transmission with cost involved in transmitting the data packet.

It should be understood that for normal circumstances, the gain involved in making data transmission is anticipated to be more than cost involved for doing the same. This process maps with both the normal nodes and malicious nodes as well. This is also the empirical form of A_1 action that could be mimicked by both malicious node as well as normal node in IoT. However, there is a slight difference in it. If the vulnerability probability *vul* $(=P_c)$ is found to be less than the cost involved in the data transmission i.e. *cost*(data_trans) than it represents the case of normal node itself (Line-5). In such case, the node opts for exercising A_1 action and set the highest probability p_1 as 1 (Line-6) otherwise it still chooses A_1 action but mark that node as vulnerable node with re-computation of the probability p_2. The variable p_2 is computed as difference of cost of launching an attack with cost of forwarding data packet and the entire thing is divided by profit that it makes in launching an attack (Line-8). The algorithm finally updates B_1 and B_2, while it performs updating operation of P_c and χ (Line-9). Finally, the node-A is identified as malicious node (Line-12).

One of the interesting points to be observed in proposed algorithm is that the proposed algorithm makes the source node compute the intention of the entire neighboring node. If it finds any malicious node with no intention of launching an attack than it allows that node to forward the data packet and also flag that node as malicious node. Therefore, the proposed system completely exploits the network behavioural information of all nodes, which is absolutely not at all a computationally intensive process. However, if the malicious node is found with confirmed intention to launch attack, it isolates the target malicious node immediately.

2.4. Bridging trade-off between Energy and Security

There are many ways the proposed algorithm bridges the trade-off between the energy-efficiency and leveraging security strength as follows:

2.4.1. Non-cryptographic origin

The complete implementation doesn't use any forms of encryption algorithm, which results in maximum saving of allocated power to perform recursive operation of encryption as well as decryption. The complete resistance policy is based on increasing value of vulnerability factor i.e. χ. Unlike any conventional encryption method, where the key-values will required to be saved and then processed (that consumes memory as well as energy too), the proposed system is completely independent of any such storage utilization.

2.4.2. Greedy nature of execution

Existing intrusion detection and prevention system works on the principle of identification followed by isolation of adversary. However, different from any existing security practices on IoT, the proposed system permits malicious nodes to assists in data transmission process until and unless the computed intension of the attacker node is not malicious. The ideology behind this is –any malicious node will resist them getting caught by launching attack in new environment. Hence, they assist in forwarding data packets that directy benefits the transmission process. A significant amount of extra transmittance energy is saved in this process.

2.4.3. Extremely lesser processing demands

Apart from standard requirement of data processing, the proposed algorithm doesn't have any other dependencies in order to execute this algorithm. A closer look into the algorithm will show presence of different number of parameters e.g. Pc, χ, B1, B2, etc can be extracted from any beacon headers as they are formulated directly from the information exchanged by beacons during routing process. This transactional information is also stored in any gateway node in IoT and therefore, there is no extra effort is required to retrieve this information and hence it saves lot of energy.

2.4.4. Non-conventional prevention strategy

Majority of the existing security algorithms focuses on first identification and then prevention exercise. However, prevention strategy will be required to allocate extra resources along with energy and it also depends how lethal is the attack. In short, preventional approach requires more energy as compared to the identification exercise. However, proposed system doesn't have any such logic implementation. On the basis of computation of vulnerability parameters, when the malicious node and its harmful intention are identified, it simply isolates them from existing ongoing communication and updates its entire monitoring variable to let know its neighboring nodes about the identified attacker node. Hence, a good proportional of energy is saved because of this.

2.4.5. A cost-effective secure intelligence mechanism

A closer look at the algorithmic steps shows that proposed algorithm has higher dependencies on the threshold. However, if the network becomes highly dynamic in future (by introducing different mobile platforms/nodes), it is not feasible for user to change the threshold accordingly. Because in such case of altering the threshold will be against the concept of sequential rationality. This problem can be solved if a cost effective intelligence is built up in such a way that precision, energy, and robustness is well maintained. Following steps has been adopted for this reason:

- In order to maintain precision in identifying malicious node, the proposed algorithm uses a variable for false positive U as a penalty factor. This will mean that if a normal node flags another normal node more malicious than it will be allocated U as a penalty. Therefore, a slight amendment is created for this purpose of catering up the logic of sequential rationality. In this case, the algorithm should compute $\phi(A3)>\text{argmax}\{ \phi(A1), \phi(A2) \}$ where ϕ represents anticipation function. The value of this function will be equivalent to scalar multiplication between J1 and J2,where J1 represents $Pc(1- \chi).\Delta A3$ and J2 represents$((1-Pc).(1- \chi)+ \chi).(U+cost(A3))$. The above expression of $\phi(A3)>\text{argmax}\{ \phi(A1), \phi(A2) \}$ represents a condition on when node-B should flag or update. However, if $\phi(A1)>0$, node-B should not opt for A1 action. Hence, dynamic thresholding is carried out by updating threshold as L1/L2, where L1→U+cost(A3) and L2→prof(A3)+U. Hence, when reduction in U also reduce threshold making it possible for dynamic thresholding. Hence, without using any potential amount of energy allocation, the algorithm offers intelligence building for resisting majority of threats.

2.4.6. Higher security encapsulation

Unlike any existing security algorithms that focuses on specific forms of threats, the proposed system offerssecurity against all forms of adversaries that directly or indirectly results in depletion of the energy from the IoT nodes. Therefore, without involving any extra energy consumption, the proposed system offers higher level of security towards IoT.

3. RESULT ANALYSIS

This section discusses about the results being accomplished from the proposed implementation in order to assess the security strength of the proposed system. The proposed logic discussed in prior section has been implemented with 500 IoT nodes dispersed in 1000x1200m^2 simulation area. The complete analysis was recorded for 600 simulation rounds on increasing stages of games. The analysis has been carried out considering the performance parameter of legitimacy and vulnerability factor with respect to probability of compromised IoT device. Discussion of process of calculating legitimacy as well as vulnerability factor has been briefed in prior section. For an effective analysis, the study outcome has been compared with work carried out by Agah et al. [31] and Hamdi et al. [32]. Agah et al. [31] has presented a definitive technique where each node (normal and compromised) can increase its respective capability based on its type (normal node protects and malicious node attacks). Similarly, work of Hamdi et al. [32] is slightly enhanced version of Agah et al. [31] where the system allocates probability to each node working on definitive strategy. In order to perform comparative analysis, only the core aspect of the algorithm has being implemented over the similar test-environment where the proposed system was investigated. A closer look into the outcome shows that proposed system offers reduced threats to IoT devices in increasing staged games as compared to existing system as shown in Figure 3. The prime reason behind this is existing mechanism calls for one round of check for all the nodes in communication in order to ascertain the facts of legitimacy of the node, but proposed system performs progressive strategy to monitor the malicious behaviour of compromised IoT device by using empirical value of vulnerability. Therefore, in a long run of multi-staged games, the proposed system will always reduce threat level (reduction in P_c)

A distinct performance of lowering threat level by proposed system can be seen in Figure 4 in comparison to existing system. With increasing simulation trials, the vulnerability spontaneously minimizes and hence it can be also said that the energy dissipation also minimizes too. As the proposed system considers energy being dissipated owing to energy-based attackers, so the reduction in threat level is equivalent to minimization of unwanted (or illegitimate) energy depletion. Therefore, a good balance is maintained for energy depletion due to security problems in IoT. Apart from the security strength, the proposed system is also assessed for its energy efficiency too. Figure 5 highlights the comparative analysis of the proposed system to existing system with respect to utility factor.

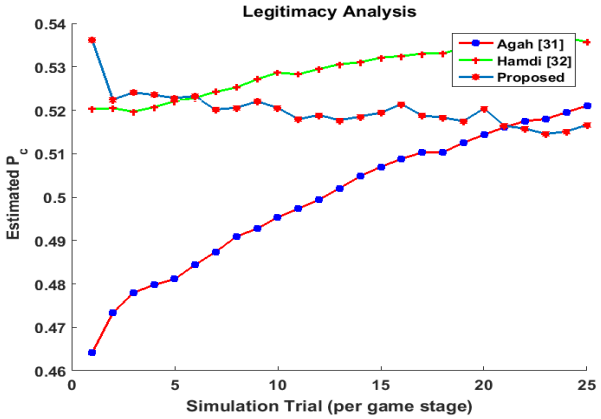

Figure 3. Comparative analysis of legitimacy

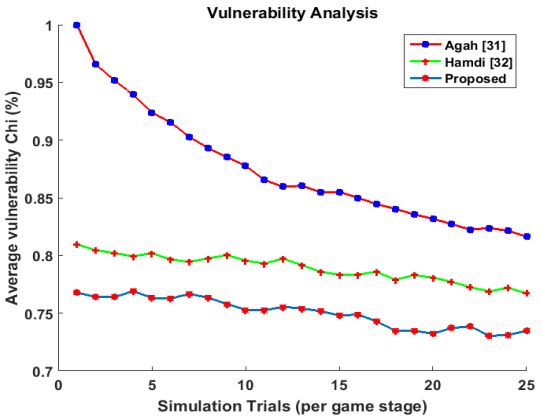

Figure 4. Comparative analysis of vulnerability

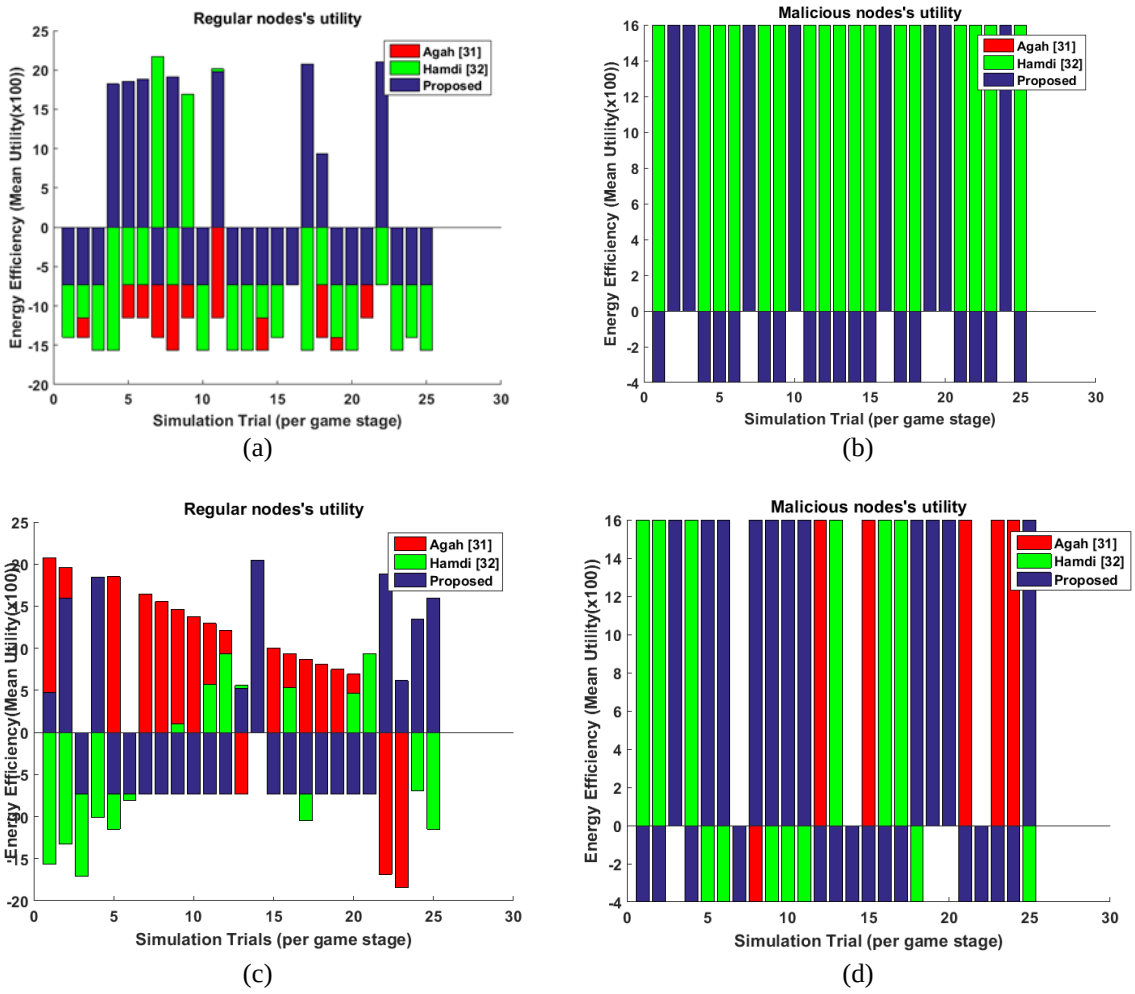

Figure 5 Comparative Analysis of Utility, (a) Regular Node Utility, (b) Malicious Node Utility, (c) Regular Node Utility, (d) Malicious Node Utility

The outcome is interpreted with respect to normal node and malicious node utility. A closer look at the utility of the regular node (Figure 5(a), (c)) shows that proposed system offers allocation of higher utility for the normal nodes as compared to the exitsing approaches. It actually means that adoption of Bayesian equilibrium concept by proposed system offers better energy efficiency as compared to Agah et al. [31] who has used definitive approach and Hamdi et al. [32] who have used opportunistic approach. Moreover, with increase of game stage (in x-axis), the outcomes looks quite practical and beneficial from resource saving too. On the otherhand, (Figure 5(b), (d)) shows that irrespective of any approach, the value of the utility for malicious node is kept constant and less than what has been received by normal node. There is a reason behind this. Looking at the difference between the utility values, it can be seen that there is a good variation with achieving higher utility value for normal node, but utility of the malicious node is not allowed to be increased for both proposed as well as existing system. However, in order to obtain this result, a single formulation of utility matrix has been carried out for all the system overlooking the utility matrix created in existing system.

Hence, the malicious node is never allocated increasing utility and this is best way to discourage any action taken by the malicious node. The best part of the implementation is if the malicious node is assisting in forwarding the data packet, there is no impact on its allocated utility by the system. However, even in compliance of sequential rationality, if the malicious node successfully launches an attack with expectation of higher profit than it is allocated with constant utility only. This concept creates further obfuscation among the malicious node by declining the idea of launching attack and accepts to forward the data packet instead. Therefore, the proposed system potentially and tacticaly manages the performance of security strength and energy efficiency.

4. CONCLUSION

A compliance of security as well as energy efficiency is highly essential especially if it is a sensor device that has limited computational capability with resource constraint. This manuscript has presented a novel approach where both detection as well as isolation of intruder node is carried out by using game theory. The interesting point of implementation is that it could offer significant security without even using any typical encryption-based security scheme. The power of sequential rationality introduced in this paper allow the normal node to increase its payoff by catching hold of attacker node while it always restricts any form of attacker node to certain ceiling of payoff. Hence, at no point of time an adversary node will be highly spending their entire resource to initiate an attack but will never be successful in its attempts. As without obtaining payoff value, the adversary cannot decide what action it should actually take. The simulation outcome of the study has proved that proposed system offers better resistance from any form of energy-depletion attacks as well as it also offers good energy efficiency in comparison to frequently exercised concepts.

REFERENCES

[1] Olof Liberg, Marten Sundberg, Eric Wang, Johan Bergman, Joachim Sachs, *Cellular Internet of Things: Technologies, Standards, and Performance*, Academic Press, 2017.

[2] Bhadoria Robin Singh, Chaudhari Narendra, Tomar Geetam Singh, Singh Shailendra, *Exploring Enterprise Service Bus in the Service-Oriented Architecture Paradigm*, IGI Global, 2017

[3] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security—A Survey," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, Dec 2017.

[4] S. Benzarti, B. Triki and O. Korbaa, "A survey on attacks in Internet of Things based networks," *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, 2017, pp. 1-7.

[5] D. M. Mena, I. Papapanagiotou, B. Yang, "Internet of things: Survey on security," *Journal of Information Security Journal: A Global Perspective*, vol. 27, no. 3, 2018.

[6] M. Sain, Y. J. Kang, H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, 2017, pp. 699-704.

[7] R. Benabdessalem, M. Hamdi and T. H. Kim, "A Survey on Security Models, Techniques, and Tools for the Internet of Things," *2014 7th International Conference on Advanced Software Engineering and Its Applications*, Haikou, 2014, pp. 44-48.

[8] V. Shakhov, I. Koo and A. Rodionov, "Energy exhaustion attacks in wireless networks," *2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)*, Novosibirsk, 2017, pp. 1-3.

[9] F. Jalali, S. Khodadustan, C. Gray, K. Hinton and F. Suits, "Greening IoT with Fog: A Survey," *2017 IEEE International Conference on Edge Computing (EDGE)*, Honolulu, HI, 2017, pp. 25-31.

[10] Baoqiang Kan, Li Cai and Lei Zhao, "An accurate energy model for wsn node and its optimal design," *2007 International Conference on Communications, Circuits and Systems*, Kokura, 2007, pp. 328-332.

[11] Wolf, Marilyn, and Dimitrios Serpanos. "Safety and security in cyber-physical systems and Internet-of-Things systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 9-20, 2018.

[12] E. Bertino, N. Islam, "Botnets and Internet of Things Security," in *Computer*, vol. 50, no. 2, pp. 76-79, Feb 2017.

[13] Singh, Jatinder, *et al.*, "Twenty security considerations for cloud-supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269–284, Jun 2016.

[14] S. Bhattarai and Y. Wang, "End-to-End Trust and Security for Internet of Things Applications," in *Computer*, vol. 51, no. 4, pp. 20-27, Apr 2018.

[15] A. Burg, A. Chattopadhyay and K. Y. Lam, "Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things," in *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38-60, Jan 2018.

[16] J. R. C. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems," in *IT Professional*, vol. 19, no. 5, pp. 20-26, 2017.

[17] Szymanski Ted H., "Security and privacy for a green Internet of Things," *IT Professional*, vol. 19, no. 5, pp. 34-41, 2017.

[18] Xu Guangquan, *et al.*, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046-21056, 2017.

[19] Y. Liu, Y. Kuang, Y. Xiao and G. Xu, "SDN-Based Data Transfer Security for Internet of Things," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 257-268, Feb 2018.

[20] Villari Massimo, *et al.*, "Software defined membrane: policy-driven edge and Internet of Things security," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 92-99, 2017.

[21] M. A. Mughal, X. Luo, A. Ullah, S. Ullah and Z. Mahmood, "A Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things," in *IEEE Access*, vol. 6, pp. 31630-31643, 2018.

[22] Pereira Geovandro CCF, *et al.*, "Performance evaluation of cryptographic algorithms over IoT platforms and operating systems," *Security and Communication Networks 2017*, 2017.

[23] Raza Shahid, *et al.*, "S3K: scalable security with symmetric keys—DTLS key establishment for the Internet of things," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1270-1280, 2016.

[24] Xiao Dianyan and Yang Yu, "Cryptanalysis of Compact-LWE and Related Lightweight Public Key Encryption," *Security and Communication Networks 2018*, 2018.

[25] Song Wei-Tao, Bin Hu and Xiu-Feng Zhao, "Privacy Protection of IoT Based on Fully Homomorphic Encryption," *Wireless Communications and Mobile Computing 2018*, 2018.
[26] H. Wu and W. Wang, "A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1432-1445, Jun 2018.
[27] L. Hu, *et al.*, "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," in *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219-228, Feb 2018
[28] N. Moustafa, E. Adi, B. Turnbull and J. Hu, "A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems," in *IEEE Access*, vol. 6, pp. 32910-32924, 2018
[29] Qu Chao, *et al.*, "Blockchain Based Credibility Verification Method for IoT Entities." *Security and Communication Networks 2018*, 2018.
[30] O. Alsaryrah, I. Mashal and T. Y. Chung, "Bi-Objective Optimization for Energy Aware Internet of Things Service Composition," in *IEEE Access*, vol. 6, pp. 26809-26819, 2018.
[31] A. Agah, S. K. Das and K. Basu, "A game theory based approach for security in wireless sensor networks," *IEEE International Conference on Performance, Computing, and Communications 2004*, 2004, pp. 259-263.
[32] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 920-925.
[33] M. Mozaffari, W. Saad, M. Bennis and M. Debbah, "Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574-7589, Nov 2017.
[34] S. S. Roy, D. Puthal, S. Sharma, S. P. Mohanty and A. Y. Zomaya, "Building a Sustainable Internet of Things: Energy-Efficient Routing Using Low-Power Sensors Will Meet the Need," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 42-49, Mar 2018.
[35] K. Shafique, *et al.*, "Energy Harvesting Using a Low-Cost Rectenna for Internet of Things (IoT) Applications," in *IEEE Access*, vol. 6, pp. 30932-30941, 2018.
[36] M. Bisadi, A. Akrami, S. Teimourzadeh, F. Aminifar, M. Kargahi and M. Shahidehpour, "IoT-Enabled Humans in the Loop for Energy Management Systems: Promoting Building Occupants' Participation in Optimizing Energy Consumption," in *IEEE Electrification Magazine*, vol. 6, no. 2, pp. 64-72, Jun 2018.
[37] A. Caruso, S. Chessa, S. Escolar, X. del Toro and J. C. López, "A Dynamic Programming Algorithm for High-Level Task Scheduling in Energy Harvesting IoT," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2234-2248, June 2018.
[38] D. Casado-Mansilla, *et al.*, "A Human-Centric & Context-Aware IoT Framework for Enhancing Energy Efficiency in Buildings of Public Use," in *IEEE Access*, vol. 6, pp. 31444-31456, 2018.
[39] D. Zhai, R. Zhang, L. Cai, B. Li and Y. Jiang, "Energy-Efficient User Scheduling and Power Allocation for NOMA-Based Wireless Networks With Massive IoT Devices," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1857-1868, Jun 2018.
[40] Q. Ju, H. Li and Y. Zhang, "Power Management for Kinetic Energy Harvesting IoT," in *IEEE Sensors Journal*, vol. 18, no. 10, pp. 4336-4345, May 2018.
[41] Sara Riahi, Azzeddine Riahi, "Game theory for resource sharing in large distributed systems," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 2, pp. 1249-1257, 2019.
[42] Sahnoun, Abdelkabir, Ahmed Habbani, and Jamal El Abbadi, "A Coalition-Formation Game Model for Energy-Efficient Routing in Mobile Ad-hoc Network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 1, pp. 26-33, 2018.
[43] Ahuja Rakesh and S. S. Bedi, "Robust Video Watermarking Scheme Based on Intra-Coding Process in MPEG-2 Style," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 7, no. 6, pp. 2088-8708, 2017.

BIOGRAPHIES OF AUTHORS

Bhagyashree Ambore completed her B.E in Computer Science and Engineering in 2006 and M.Tech in Computer Science and Engineering in 2012 and awarded as "young Investigator". Currently she is pursuing her PhD in computer science and Engineering from Visvesvaraya Technological University. She is working as Assistant Professor in the Department of Computer Science and Engineering at Cambridge Institute of Technology, Bangaluru. She has more than 7 years of experience in teaching.

Suresh L Obtained his B.E degree in Computer Science and Engineering from GIT Belagum, Karnataka University in 1990 and M.E in Computer Science and Engineering in St. Peter's University, Chennai. He received Ph.D degree in Computer Science and Engineering in 2010. Right from 1990 he is working in the Department of Computer Science & Engineering under various designations. Presently he is working as Principal and Professor in Department of Computer Science and Engineering at Cambridge Institute of Technology, Bengaluru. He has more than 28 years of experience.